UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/587,932	06/06/2000	Xin Qiu	18926-002310US	8876

20350 7590 12/15/2004

TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER	
SON, LINH L D	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 12/15/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/587,932	QIU ET AL.	
	Examiner	Art Unit	
	Linh Son	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 June 2000*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *10/30/2000*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This written action is responding to the Amendment received on June 22nd of 2004.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1-5, and 7-9 are rejected under 35 U.S.C. 102(e) as being anticipated by Chan, US Patent No. 6609202B1, hereinafter '202.

4. As per claim 1, " a method of providing data, said method comprising: storing a first set of encryption data associated with a first data stream; encrypting a first data stream having said first-level-of-encryption; sending said first data stream to a destination device for decryption" is taught in '202 (Col 13 lines 10-

15 and Col 10 lines 29-40); "storing a second set of encryption data associated with a second data stream; encrypting the second data stream having a second-level-of-encryption, said first-level-of-encryption being different from said second-level-of-encryption" is taught in '202 (Col 13 lines 17-21 and Col 11 lines 62-67); "utilizing a common memory to encrypt said first data stream at said first level-of-encryption and to encrypt said second data stream at said second-level-of encryption; sending said second data stream to said destination device for decryption" is taught in '202 (Col 13 lines 10-21, Col 4 lines 20-35, and Col 11 lines 37-43 and lines 62-67).

5. As per claim 2, "the method as described in claim 1 wherein said first set of encryption data comprises at least one encryption key" is taught in '202 (Col 2 lines 5-10).

6. As per claim 3, "the method as described in claim 1, wherein said destination device comprises a set top box" is taught in '202 (Col 4 lines 5-10 and lines 45-52).

7. As per claim 4, "the method as described in claim 3 and further comprising storing a plurality of decryption algorithms at said set-top box" is taught in '202 (Col 4 lines 35-45, and Col 10 lines 29-40).

8. As per claim 5, "the method as described in claim 1 and further comprising: transmitting a first number of services in said first data stream; and transmitting a second number of services in said second data stream, said second number of services being different from said first number of services" is taught in '202 (Col 13 lines 10-20).

9. As per claim 7, "the method as described in claim 1 and further comprising: decrypting said first data stream at said set-top box; and decrypting said second data stream at said set-top box" is taught in '202 (Col 10 lines 29-40).

10. As per claim 8, " the method as described in claim 1 and further comprising storing a portion of said first set of encryption data in RAM" is taught in'202 (Col 10 lines 29-40).

11. As per claim 9, "the method as described in claim 1 and further comprising storing a portion of said first set of encryption data in a register of a microprocessor" is taught in '202 (Col 10 lines 29-40).

Claim Rejections - 35 USC § 103

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

13. Claims 10-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over '202.

14. As per claims 10-11 and 14, "a cryptography circuit comprising: a memory operable to store a first set of encryption data for an incoming data stream; and stores a second a second set of encryption data different from said first set of encryption data fur use in encrypting said incoming data stream" is taught in '202 (Col 13 lines 1-20 and Col 4 lines 25-29). However, "the reconfiguration circuit operable to reconfigure said memory to accommodate the new set of data for encryption" is not specifically explained in '202. Nevertheless, "there are steps of encrypting different sets of data with different levels of encryption " is taught in '202 (Cited above). Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to realize that the reconfiguration circuit operable to reconfigure said memory is taught in '202 in order to encrypt different set of data efficiently and correctly.

15. As per claim 12, "the cryptography circuit as described in claim 10 and further comprising a memory to store a plurality of encryption algorithms" is taught in '202 (Col 4 lines 26-34, and Col 11 lines 62-67)

16. As per claim 13, "the cryptography circuit as described in claim 10 wherein said reconfiguration circuit for storing a second set of encryption data; and means for implementing an encryption algorithm" is taught in '202 (Col 13 lines 10-20, and Col 11 lines 15-25). However, "the code means for storing a second set of encryption data and code means for implementing an encryption algorithm" is not specifically taught in '202. Nevertheless, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to realize that the code means could also be implemented in order to reconfigure the memory and to apply a new encryption algorithm for the second set of data.

17. As per claim 15, "the method as described in claim 14 and further comprising detecting that said second-level-of-encryption of said second data stream is different from said first-level-of-encryption of said first data stream" is taught in '202 (Col 11 lines 15-25 and lines 37-45, and Col 10 lines 29-40). Since, each data stream have different predetermined security, the encryption circuit will automatically know which level of encryption to use.

18. As per claims 16 and 17, "the method as described in claim 14 wherein said allocating a memory with a first set of decryption data corresponding to said first-level-of-encryption comprises storing decryption key data; said memory with a second set of decryption data corresponding to said second-level-of

encryption comprises storing decryption key data" is taught in '220 (Col 10 lines 29-40 and Claim 14's rejection basis).

19. As per claim 18, "the method as described in claim 14 wherein said first data stream is comprised of a plurality of different services, each service encrypted at the same level of encryption" is taught in '202 (Col 11 lines 37-45).

20. As per claim 19, "an integrated circuit comprising: an input to receive data; a memory to store a first set of cryptographic data; a processor operable to re-allocate said memory so as to store a second set of cryptographic data" is taught in '202 (Col 13 lines 10-20 and also see claim 10' basis of rejection); "wherein said processor is operable to implement a plurality of cryptographic algorithms" is taught in '202 (Col 11 lines 37-44 and lines 63-67); "a transmitter operable to transmit a data stream to a destination device, wherein said data stream comprises data encrypted according to a first cryptographic algorithm of said plurality of cryptographic algorithms and data encrypted according to a second cryptographic algorithm of said cryptographic algorithms" is taught in '202 (Col 11 lines 15-25, and Col 13 lines 10-20).

21. As per claim 20, "the integrated circuit as described in claim 19 wherein said cryptographic algorithms are encryption algorithms (Col 11 lines 37-44 and lines 63-67).

22. As per claim 21, "the integrated circuit comprising: an input to receive an incoming data stream; a memory to store a first set of cryptographic data" is taught in '202 (Col 10 lines 29-40); "a processor operable to re-allocate said memory so as to store a second set of cryptographic data" is taught in '202 (See Claim 14's rejection basis); "wherein said processor is operable to implement a plurality of cryptographic algorithms so as to decrypt a first portion of said incoming data stream according to a first cryptographic algorithm of said plurality of cryptographic algorithms and so as to decrypt a second portion of said incoming data stream according to a second cryptographic algorithm of said plurality of cryptographic algorithm" is taught in '202 (Col 9 lines 55-65, Col 10 lines 29-40, Col 11 lines 37-44 and lines 63-67, and Col 13 lines 10-20).

23. As per claim 22, "a set-top box apparatus comprising: an input to receive a data stream; a processor coupled to said input; a memory coupled to said processor configured to store a first set of decryption data" is taught in '202 (Col 3 lines 50-63, and Col 10 lines 29-40); "code for use by said processor that allows said processor to reconfigure said memory with a second set of decryption data (See Claim 13's rejection basis, Col 10 lines 29-40, and Col 13 lines 15-20); "code for use by said processor that allows said processor to utilize said first set of decryption data to decrypt a first portion of said incoming data stream; and code for use by said processor to utilize said second set of

decryption data to decrypt a second portion of said incoming data stream" is taught in '202 (See Claim 13's rejection basis).

24. As per claim 23, "a method of providing encrypted data, said method comprising: providing a first set of services; encrypting at least one of said services from said first set of services at a first-level-of-encryption; combining the first set of services into a first data stream; transmitting from a head end to a set-top box said first data stream" is taught in '202 (Col 13 lines 10-15, and Col 10 lines 29-40); "storing a first set of decryption keys associated with said first-level-of encryption in an integrated circuit in said set-top box, said first set of keys corresponding to the decryption algorithm for the first-level-of-encryption; decrypting said first data stream" is taught in '202 (Col 10 lines 29-40); "providing a second set of services; encrypting at least one of said services from said second set of services with an encryption algorithm different from said first-level-of-encryption; combining the second set of services into a second data stream; formatting said second data stream; transmitting from said head end to said set-top box said second data stream; storing a second set of decryption keys associated with said second-level of-encryption in said integrated circuit in said set-top box; storing a plurality of decryption algorithms in said set-top box; and decrypting said second data stream" is taught in '202 (Col 13 lines 15-20, Col 10 lines 29-40, and Col 11 lines 37-67). However, the set-top-box is not directly claimed in '202.

Nevertheless, the client secure processor in '202 can also be interpreted as a set-top-box. Therefore, it would have been obvious for one having ordinary skill in the art to modify the invention to utilize the set-to-box to provide a user friendly environment for customer to receive digital data sent from the providers.

25. **Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over '202, in view of Matthews, JR. et al, US Publication No. 20030005292A1, hereinafter '292.**

26. As per claim 6, "the method as described in claim 1 wherein said first-level of encryption utilizes the Data Encryption Standard" is taught in '202 (Col 6 lines 36-37). The second-level-of encryption is taught in '202 (Col 11 lines 37-45 and lines 63-67). However, " said second-level-of encryption utilizes an encryption algorithm different from said Data Encryption Standard" is not taught specifically. Nevertheless, the implementation of different encryption algorithm other than DES and concurrently with DES to protect the data is well known in the distribution of digital data domain and taught in '292 (Para 0019). Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify '202 invention to implement different encryption algorithm in the second-level of security other than DES to best protect the data stream.

Response to Amendment

27. Applicant has amended claims 1, 10, 14, 19, 21, and 22, which necessitated new grounds of rejection. See rejections above.

Conclusion

28. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

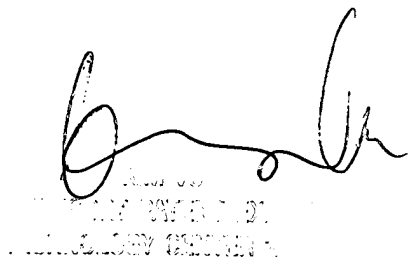
29. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Conclusion

30. Any inquiry concerning this communication from the examiner should be directed to Linh Son whose telephone number is (571)-271-3856.

31. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor Kim Y. Vu can be reached at (571)-272-3859. The fax numbers for this group are (703)-872-9306 (official fax). Any inquiry of general nature or relating to the status of this application or proceeding should be directed to the group receptionist whose telephone number is (571)-272-2100.

32. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval IPAIR.I system. Status information for published applications may be obtained from either Private PMR or Public PMR. Status information for unpublished applications is available through Private PMR only. For more information about the PAIR system, see http://pzr-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Linh LD Son

Patent Examiner